An Introduction to Stone Duality

Preliminary Notes for the MGS, 29th March – 2nd April 2004

Alexander Kurz
Department of Computer Science, University of Leicester, UK
kurz@mcs.le.ac.uk

April 9, 2004

Abstract

The aim of the course is to provide a first introduction to Stone duality. We prove two classical theorems, Stone's theorem representing Boolean algebras as topological spaces and Goldblatt's theorem representing modal algebras (Boolean algebras with operators) as topological Kripke frames (descriptive general frames).

Note: I will produce a (slightly) revised version of the notes shortly after the course (send me an email if you are interested). Any help in improving them is more than welcome! I hope to replace them then later by a more complete and self-contained version.

1 Introduction

The aim of this course is to give a basic introduction to Stone duality in Section 2. In Section 3, we make use of coalgebras (and the duality of algebras and coalgebras) in order to explain how Stone duality applies to modal logics. Two appendices recall some background on coalgebras (Appendix A) and modal logic (Appendix B).

In the remainder of the introduction we summarise the framework in which the approach of these notes applies. We only consider modal logics that are determined by adding some (possibly n-ary) modal operators to a given propositional logic.

We assume that this propositional logic comes with an associated category of algebras $\mathcal{A}$ having free algebras and providing the algebraic semantics of the propositional logic. An element of an algebra corresponds to an equivalence class of formulae under logical equivalence. For example, for classical propositional logic $\mathcal{A}$ will be the category BA of Boolean algebras.

We also assume that there is a category $\mathcal{X}$ of spaces X providing a set-based semantics of the propositional logic in which formulae correspond to subsets of X. Algebraic and set-based semantics are related by two (contravariant) functors

$$\mathcal{X} \underset{S}{\overset{P}{\rightleftarrows}} \mathcal{A}$$

P assigns to a space X the algebra of predicates over X; PX can also be understood as the logic of X. S assigns to an algebra A its space of points. SA can be understood as the canonical model of the logic A. The elements of A correspond to subsets of (ie predicates over) SA and the points of SA are given by certain complete theories ('states of affairs') of A.

That $\mathcal{X}$ and $\mathcal{A}$ are dual categories means that PS and SP are (up to natural isomorphism) the identities. Examples of such Stone dualities are given by the pairs of categories described informally by (sets, complete atomic Boolean algebras), (Stone spaces, Boolean algebras), (sober spaces, spatial frames), (spectral spaces, bounded distributive lattices), see eg [19, 2] for details and more examples.

Important for us is that, in logical terms, Stone duality implies the following three properties:

- the logic is sound
- the logic is complete
- the logic is expressive, or, equivalently, the semantic is fully abstract

The picture can be extended from categories $\mathcal{X}$ and $\mathcal{A}$ to endofunctors on these categories. Suppose we have a functor T on a category $\mathcal{X}$. We say that the functor L on $\mathcal{A}$ is the Stone dual of T if the diagram

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{P} & \mathcal{A} \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle L} \\ \mathcal{X} & \xrightarrow{P} & \mathcal{A} \end{array}$$

commutes (up to natural isomorphism).

In that case, the categories of L-algebras and T-coalgebras are also dual. Here, L encodes the modal operators and their axiomatisation of a modal logic built on top of the propositional logic corresponding to $\mathcal{A}$. T-coalgebras provide the canonical transition system semantics for this modal logic. As above, due to the duality, one immediately obtains soundness, completeness, and full abstraction.

Literature

Stone duality was introduced by Stone [36]. The application of Stone duality to modal logic goes back to J'onsson and Tarski [20, 21] and then Goldblatt [14]. The idea of relating type constructors on algebras (see the L above) and topological spaces (see the T above) is from Abramsky's Domain Theory in Logical Form [1].

Compared to [1], the approach of Section 3 is a simplification in the sense that it only deals with endofunctors T (thus excluding function space) and a generalisation in that it works for a larger class of topological spaces. Moreover, the models we are interested in are not only solutions to recursive domain equations (final coalgebras) but any coalgebras. Compared to [14], we use the duality of algebras and coalgebras to lift the Stone duality from Boolean logic to modal logic.

The main reference for Stone duality is Johnstone's book on Stone Spaces [19] which also provides detailed historical information. The handbook article [2] covers the topic from the point of view of domain theory.

I know of three introductory textbooks on the subject, all of which I find very helpful and complementing each other: Vickers [39], Davey and Priestley [11], Brink and Rewitzky [8]. A further interesting source is Bonsangue's thesis [7] which extends the duality between sober spaces and spatial frames to a duality for all T0-spaces and discusses applications to the semantics of programming languages.

My own interest in the subject is motivated by investigating the relationship between coalgebras and modal logic. The standard reference on coalgebras is Rutten's [33]. Recent textbooks on modal logic include [9, 22, 6]. Coalgebras and modal logic has attracted the attention of several researcher, see Moss [29] for the original paper and eg [32, 18, 4, 31, 16, 10] for further work. The course notes [26] provide an introduction and overview. [25, 30, 24, 27] is recent work building on the ideas explained in Section 3.

2 Stone Duality

2.1 Representation of Boolean Algebras

Definition 2.1 (Distributive lattices, Boolean algebras). A lattice has constants $0, 1$ and binary operators $\vee, \wedge$. Each of $\vee, \wedge$ is associative, commutative and idempotent, and $0, 1$ are the neutral elements for $\vee, \wedge$, respectively. Moreover,

$$a \vee (a \wedge b) = a \qquad a \wedge (a \vee b) = a$$

A lattice is distributive if it satisfies

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \qquad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

A Boolean algebra is a distributive lattice with an additional unary operation $\neg$ such that

$$a \wedge \neg a = 0 \qquad a \vee \neg a = 1$$

The categories of distributive lattices and Boolean algebras are denoted by DL and BA, respectively. The set of equations defining Boolean algebras is denoted by E_{BA}.

Remark 2.2. A lattice can also be defined as a poset that has finite joins (least upper bounds) and finite meets (greatest lower bounds). The definition above has the advantage of exhibiting distributive lattices as algebras given by a signature and equations. The poset order can be recovered via $a \leq b \Leftrightarrow a \wedge b = a$.

The prototypical example of Boolean algebras is the following.

Definition 2.3. A field of sets is a subset $A \subseteq \mathcal{P}X$ for some set X such that A is closed under finite unions, finite intersections and complements. In other words, $(A, \emptyset, X, \cup, \cap, -)$ is a Boolean algebra.

That the abstract[1] equations defining Boolean algebras (Definition 2.1) indeed completely capture the properties of union, intersection and complement is the content of the following theorem.

Theorem 2.4. *Any boolean algebra is isomorphic to a field of sets.*

Given a boolean algebra A, we have to describe an isomorphic algebra whose *elements are subsets* of a set (of 'points') $Pt(A)$. The crucial question is how to find this set of points $Pt(A)$. Before we do this, it may be helpful to look, for additional motivation, at a similar, but perhaps more intuitive problem.

[1]'Abstract' means here that even though we might want to think of the elements of a Boolean algebra as sets, the elements of these sets do not play a role in the axiomatisation of Boolean algebras.

Example 2.5 (Constructing time-points from time-intervals).

The set of points $Pt(A)$ will consist of subsets of A, or, equivalently, of functions $A \to 2$. Thinking about which functions $A \to 2$ we should consider as points (in terms of the example above: not all sets of intervals are good), there is one obvious choice. Indeed, 2 is not only a set, but also a boolean algebra, denoted $\mathbb{2}$. This suggests to define

$$Pt(A) = \mathsf{BA}(A, \mathbb{2}).$$

Each element a of A can be represented by $\hat{a} \subseteq Pt(A)$

$$\hat{a} = \{p \in Pt(A) \mid p(a) = 1\}.$$

Note that the idea that the point p satisfies the 'predicate' a can now be expressed naturally as $p \in \hat{a}$. To finish the construction of the field of sets $\hat{A}$ corresponding to the boolean algebra A we let

$$\hat{A} = \{\hat{a} \mid a \in A\}$$

and the boolean operators be the set-theoretic ones. That $\hat{A}$ is indeed isomorphic to A depends on the following

Lemma 2.6. *The map*

$$\begin{aligned} \hat{(\cdot)} : A &\longrightarrow \mathcal{P}Pt(A) \\ a &\mapsto \hat{a} \end{aligned}$$

is an injective boolean algebra morphism.

2.2 Duality for Finite Boolean Algebras

Fin denotes the category of finite sets and functions.

Theorem 2.7. *The categories* $\mathsf{Fin}^{\mathrm{op}}$ *and* $\mathsf{BA}_{\mathsf{fin}}$ *are equivalent.*

Proof. Homework 1. Hint: Every finite Boolean algebra is atomic, that is, every element is a join of atoms (where a is an atom if $0 \leq b < a \Rightarrow b = 0$). □

2.3 The Logical Interpretation of the Representation Theorem

$\vdash \varphi$

propositional logic is algebraisable

$E_{\mathsf{BA}} \vdash \varphi = 1$

soundness and completeness of equational logic

$\mathsf{BA} \models \varphi = 1$

representation theorem

$\mathit{FieldOfSets} \models \varphi = 1$

If we don't want to take the set-theoretic interpretation of the operators as our semantics but prefer to rely on the usual truth table definition, we can continue:

$\mathit{FieldOfSets} \models \varphi = 1$

every set-algebra is a subalgebra of a product of 2s

$2 \models \varphi$

'truth-table' definition of $\models$

$\models \varphi$

2.4 Stone Duality: the Topological Interpretation of the Representation Theorem

In this section we sharpen the represenation theorem to a *duality* between the category of Boolean algebras BA and a certain category of topological the spaces, the category Stone of Stone spaces.

First, we describe the category RBA (represented boolean algebras which is not standard terminology) that consists of those fields of sets that arise as representations of Boolean algebras.

Definition 2.8 (RBA)**.** RBA consists of objects (X, A) where X is a set and $A \subseteq \mathcal{P}X$ is a Boolean subalgebra of $\mathcal{P}X$. Moreover, (X, A) has to be

1. *differentiated*, that is, for all $x \neq x'$ in X there is a in A containing x but not x',

2. *compact*, that is, if $\bigcup_{i \in I} a_i = X$ then there is a finite subset J of I such that $\bigcup_{i \in J} a_i = X$.

A morphism $f : (X, A) \to (Y, B)$ is a function $f : X \to Y$ such that $f^{-1}(b) \in A$ for all $b \in B$ (in other words, f^{-1} is a Boolean algebra morpism $B \to A$).

In this terminology, the representation theorem gives us a contravariant functor

$$S : \mathsf{BA} \longrightarrow \mathsf{RBA}$$
$$A \mapsto (Pt(A), \hat{A})$$

which together with the contravariant functor

$$P : \mathsf{RBA} \longrightarrow \mathsf{BA}$$
$$(X, A) \mapsto A$$

and the natural transformations

$$\rho_A : A \longrightarrow \hat{A}$$
$$a \mapsto \hat{a}$$

and

$$\sigma_{(X,A)} : (X, A) \longrightarrow (Pt(A), \hat{A})$$
$$x \mapsto p_x = \{a \in A \mid x \in a\}$$

forms an adjunction (Check: $S\rho_A \circ \sigma_{SA} = id_{SA}$, $P\sigma_{X,A} \circ \rho_{P(X,A)} = id_{P(X,A)}$). Moreover this adjunction is a duality (or, dual equivalence) because the natural transformations are isomorphisms. To summarise:

Proposition 2.9. *The categories* BA *and* RBA *are dually equivalent. The duality is induced by the contravariant functor* $\mathsf{BA} \to \mathsf{RBA}$ *mapping a Boolean algebra to its set-theoretic representation.*

This is essentially the duality theorem we have been aiming for. To make the connection with topology we just have to note that represented Boolean algebras are nothing but Stone spaces in disguise.

Definition 2.10 (Stone space)**.** A toplogical space is a Stone space if it is Hausdorff, compact, and has a basis of clopens. Stone is the category of Stone spaces and continuous maps.

Given (X, A) in RBA, we let $\mathcal{O}X$ be the closure of A under arbitrary unions. This is Hausdorff since (X, A) is differentiated, compact since (X, A) is compact and has a basis of clopens because A is a Boolean algebra. That, conversely, every Stone spaces arises in this way depends on the following lemma.

Lemma 2.11. *If a topological space is compact and has a basis* A *of clopens that is closed under Boolean operations, then* A *contains all clopens.*

In other words, in the presence of compactness, there is only one basis of clopens that is a Boolean algebra under the set-theoretic operations. Compactness is essential here. For example, the topological space $(\mathbb{N}, \mathcal{P}\mathbb{N})$ has two different such basises of clopens, one being $\mathcal{P}\mathbb{N}$ itself and the other consisting of the finite subsets and their complements. As a corollary to the lemma we get the next two statements.

Proposition 2.12. Stone *and* RBA *are (concretely) isomorphic categories.*

Theorem 2.13 (Stone duality for Boolean algebras)**.** Stone *and* BA *are dual categories.*

Proof. Immediate from Propositions 2.9 and 2.12. □

2.5 Stone Duality for Distributive Lattices

Definition 2.14 (spectral space)**.** A toplogical space $(X, \mathcal{O}X)$ is a spectral space if it is sober, each open is a union of compact opens, and the collection of all compact opens forms a distributive lattice. Spec is the category of spectral spaces and those continuous maps that preserve compact opens.

Theorem 2.15 (Stone duality for distributive lattices)**.** Spec *and* DL *are dual categories.*

Proof. Homework 2. Follows the same lines as layed out for Boolean algebras. □

3 Stone duality and modal logic

As explained in the introduction, the idea is to extend a Stone duality

$$\mathcal{X} \underset{S}{\overset{P}{\rightleftarrows}} \mathcal{A}$$

for a basic propositional logic to a duality for a modal logic via two dual functors

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{P} & \mathcal{A} \\ {\scriptstyle T}\big\downarrow & & \big\downarrow{\scriptstyle L} \\ \mathcal{X} & \xrightarrow{P} & \mathcal{A} \end{array}$$

The L-algebras $\mathsf{Alg}(L)$ describe (the algebraic semantics of) the modal logic and the T-coalgebras describe the (relational or coalgebraic) semantics of the modal logic.

The duality amounts to saying that the logic is sound and complete and that the semantics is fully abstract (or that the logic is expressive up to bisimulation).

3.1 Algebraisation of modal logic

Abstract algebraic logic associates to each logic a canonical class of algebras [13]. Here we only look at one example, namely the (basic) modal logic $\mathcal{ML}$ (see Appendix B). $\mathcal{ML}$ is algebraisable in the following sense.

There is a signature Σ (Boolean operations plus one unary operator $\Box$) and a set of equations E ($\Box$ preserves finite meets) and there are (definable) operators 1 and $\leftrightarrow$ such that

$$\vdash_{\mathcal{ML}} \varphi \;\Leftrightarrow\; E_{\mathsf{BA}} + E \vdash_{\mathcal{EL}} \varphi = 1 \tag{1}$$

$$E_{\mathsf{BA}} + E \vdash_{\mathcal{EL}} \varphi = \psi \;\Leftrightarrow \vdash_{\mathcal{ML}} \varphi \leftrightarrow \psi \tag{2}$$

Now define a **modal algebra**[2] as a set of modal formulae closed under Boolean and modal operators and quotiented by logical equivalence (two terms φ and ψ are logically equivalent iff $\vdash_{\mathcal{ML}} \varphi \leftrightarrow \psi$ (Exercise: check that logical equivalence is a congruence). It now follows from (1) and (2) that modal algebras are precisely the Σ-algebras satisfying the equations E_{BA} and E.

The fact that the axioms of modal logic are only of 'depth one' corresponds to the fact that modal algebras are algebras for a functor on Boolean algebras. For details of how to represent algebras by generators and relations see [39].

[2] Also known as *Boolean algebra with operator* (BAO).

Proposition 3.1. *The category of modal algebras is isomorphic to the category of algebras for the functor*

$$L : \mathsf{BA} \longrightarrow \mathsf{BA}$$

that maps a Boolean algebra A to the free Boolean algebra generated by $\{\Box a : a \in A\}$ quotiented by the smallest congruence containing $(\Box 1, 1)$ and $(\Box a \wedge \Box b, \Box(a \wedge b))$, $(a, b \in A)$.

3.2 From algebraic to coalgebraic semantics

The functor dual to L is known as Vietoris functor, or, in domain theory, as the Plotkin powerdomain.

Definition 3.2. Given a Stone space X, we define $\mathcal{V}X$ as the collection of closed subsets of X. The topology on $\mathcal{V}X$ is the topology generated by all $\Box a = \{b \in \mathcal{V}X \mid b \subseteq a\}$, $a \in A$.

Proposition 3.3. *The functor L from Proposition 3.1 is dual to $\mathcal{V}$.*

Proof. Homework: Complete the proof from the lecture. □

Corollary 3.4. *The category of L-algebras is dual to the category of $\mathcal{V}$-coalgebras.*

This entails Goldblatt's duality between modal algebras and descriptive general frames as follows.

Definition 3.5. A **modal algebra** is a Boolean algebra with an additional finite-meet preserving operation (usually denoted $\Box$).

Definition 3.6. A **general frame** is a structure (X, R, A) such that (X, R) is a Kripke frame and A is a collection of so-called *admissible* subsets of X that is closed under the boolean operations and under the operation $\Box_R : \mathcal{P}X \to \mathcal{P}X$ given by: $\Box_R(Y) = \{x \in X \mid Rxy \;\Rightarrow\; y \in Y\}$.

A general frame (X, R, A) is called *differentiated* if for all distinct $s_1, s_2 \in X$ there is a 'witness' $a \in A$ such that $s_1 \in a$ while $s_2 \notin a$; *tight* if whenever t is not an R-successor of s, then there is a 'witness' $a \in A$ such that $s \in \Box_R(a)$ while $t \notin a$; and *compact* if $\bigcap A_0 \neq \emptyset$ for every subset A_0 of A which has the finite intersection property. A general frame is *descriptive* if it is differentiated, tight and compact.

A general frame morphism $f : (X, R, A) \to (X', R', A')$ is a function $X \to X'$ whose graph is a bisimulation between (X, R) and (X', R') and whose inverse image function is a Boolean algebra morphism $A' \to A$.

Theorem 3.7 (Goldblatt)**.** *The categories of modal algebras and descriptive general frames are dually equivalent.*

Proof. Homework. The hint is of course: Show that the category of modal algebras is isomorphic to the category of L-algebras and that the category of descpriptive general frames is isomorphic to the category of $\mathcal{V}$-coalgebras. $\square$

4 Homeworks

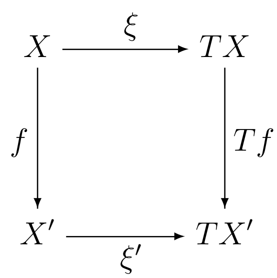
Choose one of the homeworks.[3] 2.15 is probably the most difficult because the step from Boolean algebras to distributive lattices needs some adjustments. 3.7 shouldn't be too difficult since it needs not much more than unfolding the definitions. On the other hand it is a good exercise since it involves most of the notions presented in the course, in particular it will help to understand the definition of the functor L. 2.7 is a classic that is worth doing anyway. (What is the analogue for distributive lattices?) Finally, 3.3 is also worth doing (note that it essentially amounts to proving completeness of modal logic).

[3]Numbers refer to the theorems whose missing proofs you are asked to supply.

A Algebras and Coalgebras for a Functor

This is an abbreviated version of Section 2 in [26].

Definition A.1. Given a category $\mathcal{X}$, called the base category, and a functor $T : \mathcal{X} \to \mathcal{X}$, a T-**coalgebra** (X, ξ) is given by an arrow $\xi : X \to TX$ in $\mathcal{X}$. A morphism between two coalgebras $f : (X, \xi) \to (X', \xi')$ is an arrow f in $\mathcal{X}$ such that $\xi' \circ f = Tf \circ \xi$:



The category of coalgebras and morphisms is denoted by $\mathsf{Coalg}(T)$.

We will explain in more detail what in means for the signature to be a functor. Assume $\mathcal{X} = \mathsf{Set}$. Then we have functors as follows (let $C \in \mathsf{Set}$ and $f : X \to Y \in \mathsf{Set}$):

T	TX	Tf
C	C	$id_C : C \to C$
Id	X	f
$(-)^C$	X^C	$f^C : X^C \to Y^C$ $g \mapsto f \circ g$

We overloaded notation by denoting with C the set as well as the constant functor mapping any set to C. id_C denotes the identity map on C and X^C is function space.

From these functors, we can build more interesting ones, using $\times$ and $+$, like eg $TX = (E + A \times X)^I$. [4] To make this precise, we note that $\times$ and $+$ are functors as well. Their action on functions $f_1 : X_1 \to Y_1$, $f_2 : X_2 \to Y_2$ is the following:

[4] A coalgebra $X \to (E + A \times X)^I$ can be understood as mapping a state $x \in X$ and an input $i \in I$ to either an exception $e \in E$ or an output $a \in A$ and a successor state $x' \in X$.

$-+-$	$f_1 + f_2 : X_1 + X_2 \to Y_1 + Y_2$ $x \in X_1 \mapsto f_1(x)$ $x \in X_2 \mapsto f_2(x)$
$- \times -$	$f_1 \times f_2 : X_1 \times X_2 \to Y_1 \times Y_2$ $\langle x_1, x_2 \rangle \mapsto \langle f_1(x_1), f_2(x_2) \rangle$

It is perhaps not worth looking at these definitions in detail. There are no reasonable alternatives anyway. But these definitions show that any expression build from constants, identity, exponentiation with a constant, $+$, and $\times$ gives rise to a functor (this is due to the fact that the composition of functors is a functor).

Another important example of a functor is the powerset functor $\mathcal{P}$ that allows to model non-determinism:

T	TX	Tf
$\mathcal{P}$	$\{W : W \subset X\}$	$\mathcal{P}f : \mathcal{P}X \to \mathcal{P}Y$ $W \mapsto f(W) = \{f(x) : x \in W\}$

We next characterise morphisms of $\mathcal{P}$-coalgebras. Recall that we can write a $\mathcal{P}$-coalgebra (X, ξ) as (X, R) with $R \subset X \times X$ and $x \; R \; y \;\Leftrightarrow\; y \in \xi(x)$.

Proposition A.2. *Let (X, R) and (X', R') be two $\mathcal{P}$-coalgebras. A function $f : X \to X'$ is a $\mathcal{P}$-coalgebra morphism iff*

$$x \; R \; y \;\Rightarrow\; f(x) \; R' \; f(y) \tag{3}$$

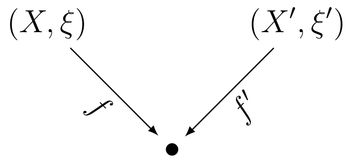
$$f(x) \; R' \; y' \;\Rightarrow\; \exists y \in X \,.\, x \; R \; y \;\&\; f(y) = y' \tag{4}$$

Proof. The commuting square defining coalgebra morphisms translates into the condition that for all $x \in X$ it holds $\{y' : f(x) \; R' \; y'\} = \{f(y) : x \; R \; y\}$. "$\supset$" is (3) and "$\subset$" is (4). □

Note that (3) says that f is a graph morphism. It expresses that $(X', R', f(x))$ simulates (X, R, x). (4) is the converse stating that (X, R, x) simulates $(X', R', f(x))$.

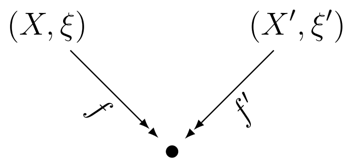
Definition A.3 (Behavioural equivalence)**.** Let (X, ξ), (X', ξ') be two coalgebras.

1. (X, ξ, x), (X', ξ', x') are behaviourally equivalent iff there are morphisms



   such that $f(x) = f'(x')$.

2. Two coalgebras (X, ξ), (X', ξ') are behaviourally equivalent iff there are surjective morphisms



The following may be no surprise but should be checked for once nevertheless.

Exercise A.4. Let T be $\mathcal{P}$ or $\mathcal{P}(A \times -)$ and (X, ξ), (Y, η) two T-coalgebras. Then $x \in X$ and $y \in Y$ are behaviourally equivalent (Definition A.3(1)) iff they are bisimilar in the usual sense of modal logic or process algebra (Definition B.10).

A.1 Final Coalgebras

An object Z in a category $\mathcal{C}$ is called **final** if for all objects $A \in \mathcal{C}$ there is a unique arrow $A \to Z$.

Proposition A.5. *Let T be an endofunctor on* Set *and assume that the final coalgebra exists in* $\mathsf{Coalg}(T)$. *Consider two coalgebras (X, ξ) and (X', ξ'). Then $x \in X$ and $x' \in X'$ are identified by the morphisms into the final coalgebra iff (X, ξ, x), (X', ξ', x') are behaviourally equivalent in the sense of Definition A.3.*

Proof. One direction is obvious. For the other use that the dijsoint union of two coalgebras is a coalgebra and that one can factor a morphism through its image.

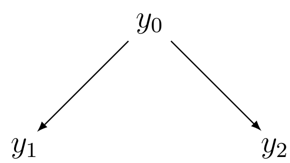
The proposition also holds if the final coalgebra exists only outside $\mathsf{Coalg}(T)$. The proof then is essentially the content of Aczel and Mendler's final coalgebra theorem [3]. □

A.2 Cofree Coalgebras

This section contains background material not needed in the present course.

We have seen that final coalgebras play an important role because they classify processes up to behavioural equivalence. *Cofree coalgebras* do the same, but allow the environment additional observations called colourings. We first take the time to discuss colourings in some detail and then explain cofree coalgebras.

Given a coalgebra $X \xrightarrow{\xi} TX$ and a set 'of colours' C, a **colouring** of (X, ξ) in C is a function $X \xrightarrow{c} C$. c is simply a marking or labeling of the states. Its import is that we can use colourings c to make additional observations. Consider eg the $\mathcal{P}_{fin}$-coalgebra (Y, η, y_0) given by



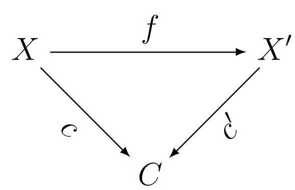
Here, the two states y_1, y_2 are behaviourally equivalent for an external observer. But allowing colourings $c : Y \to C$, $C = \{c_1, c_2\}$, an external observer can distinguish y_1, y_2 by choosing a colouring with eg $c(y_1) = c_1$ and $c(y_2) = c_2$.

That is, allowing colourings increases the observational power of the environment. If we want to stay with the paradigm that two elements cannot be distinguished by an external observer iff these elements cannot be identified by some morphisms, we need to require morphisms to respect colourings. This gives rise to a new category of coalgebras with colourings:

Definition A.6 ($\mathsf{Coalg}(T, C)$)**.** Let $T : \mathcal{X} \to \mathcal{X}$ and $C \in \mathcal{X}$. $\mathsf{Coalg}(T, C)$ is the category having objects

$$(X \xrightarrow{\xi} TX \ , \ c : X \to C)$$

where $X \xrightarrow{\xi} TX$ is a T-coalgebra and $c : X \to C$ an arrow in $\mathcal{X}$. We call these objects (T, C)-coalgebras and denote them by $((X, \xi), c)$ or (X, ξ, c). A (T, C)-morphism $f : (X, \xi, c) \to (X', \xi', c')$ is a T-morphism $(X, \xi) \to (X', \xi')$ such that



commutes.

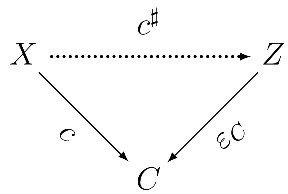
The last condition expresses that (T, C)-morphisms preserve colours.

We can now define cofree coalgebras

Definition A.7 (Cofree Coalgebras)**.** A (T, C)-coalgebra $(Z_C, \zeta_C, \varepsilon_C)$ is called the cofree T-coalgebra over C iff it is final in $\mathsf{Coalg}(T, C)$. We say that $\mathsf{Coalg}(T)$ has cofree coalgebras if cofree coalgebras exists for all $C \in \mathcal{X}$.

Usually, we leave ε_C implicit and call (Z_C, ζ_C) alone the cofree T-coalgebra over C. In the following exercise you are asked to unravel the definition of a cofree coalgebra.

Exercise A.8. Show that (Z_C, ζ_C) is cofree over C iff for all T-coalgebras (X, ξ) and all colourings $c : X \to C$ there is a unique T-morphism $c^\sharp : (X, \xi) \to (Z_C, \zeta_C)$ such that

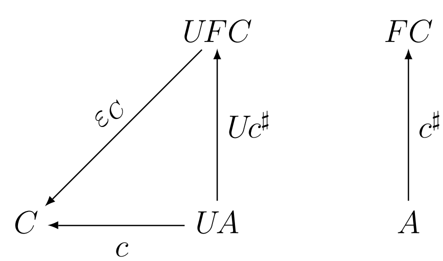


commutes.

The diagram above is not 'well-typed' in the sense that two arrows are colourings (from the base category) and another one is a coalgebra morphism. This can be corrected by introducing the following

Notation A.9 (Forgetful functor)**.** The forgetful functor is the operation $U : \mathsf{Coalg}(T) \to \mathcal{X}$ mapping a coalgebra to its carrier and a coalgebra morphism $f : (X, \xi) \to (X', \xi')$ to $f : X \to X'$.

Proposition A.10. *Let* $U : \mathsf{Coalg}(T) \to \mathcal{X}$ *be the forgetful functor.* $\mathsf{Coalg}(T)$ *has cofree coalgebras iff for each* $C \in \mathcal{X}$ *there is a* T*-coalgebra* FC *and a colouring* $\varepsilon_C : UFC \to C$ *such that for any* T*-coalgebra* A *and any colouring* $c : UA \to C$ *there is a unique coalgebra morphism* $c^\sharp : A \to FC$ *such that the triangle*



commutes.

A.3 Algebras

This section reviews algebras as far as needed to understand the duality to coalgebras. Some basic familiarity with algebras and equational logic will be helpful, see eg Wechler [40] for an introduction.

Definition A.11. Given a category $\mathcal{X}$, called the base category, and a functor $T : \mathcal{X} \to \mathcal{X}$, a T-**algebra** (Y, ν) is given by an arrow $\nu : TY \to Y$ in $\mathcal{X}$. A morphism between two algebras $(Y, \nu) \to (Y', \nu')$ is an arrow f in $\mathcal{X}$ such that $\nu' \circ Tf = f \circ \nu$:

$$\begin{array}{ccc} TY & \xrightarrow{\ \nu\ } & Y \\ {\scriptstyle Tf}\downarrow & & \downarrow{\scriptstyle f} \\ TY' & \xrightarrow[\ \nu'\ ]{} & Y' \end{array}$$

The category of T-algebras and morphisms is denoted by $\mathsf{Alg}(T)$. The forgetful functor $U : \mathsf{Alg}(T) \to \mathcal{X}$ maps algebras (Y, ν) to the carrier Y and morphisms $f : (Y, \nu) \to (Y', \nu')$ to the arrows $f : Y \to Y'$.

This notion of algebras for a functor includes algebras defined by operations in the usual sense. To give examples it is useful to have the following

Notation A.12. A family of functions $(f_i : Y_i \to Y)_{1 \leq i \leq n}$ can equivalently be written as a single function

$$Y_1 + \ldots + Y_n \xrightarrow{[f_1, \ldots, f_n]} Y$$

where as before $+$ denotes disjoint unions of sets and $[f_1, \ldots, f_n]$ is the function which applies f_i to arguments from Y_i. (This equivalence is valid in any category with coproducts.)

Example A.13. Algebras for a signatuer in the standard sense are algebras for a functor.

A T-algebra (I, ι) is **initial** iff it is initial in $\mathsf{Alg}(T)$, ie iff for any T-algebra (Y, ν) there is a unique T-morphism

$$(I, \iota) \to (Y, \nu).$$

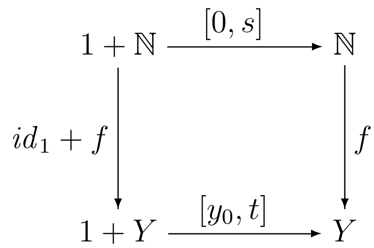
I consists precisely of all terms that can be formed from the operations in the signature. For example, the natural numbers are the initial algebra for the functor $TY = 1 + Y$ (read 0 as zero and s as successor):

$$1 + \mathbb{N} \xrightarrow{[0, s]} \mathbb{N}$$

To say that $(\mathbb{N}, [0, s])$ is initial is equivalent to the principle of **induction**. To see that initiality gives rise to induction, recall that defining a function $f : \mathbb{N} \to Y$ by induction means to give a $y_0 \in Y$ such that $f(0) = y_0$ and a $t : Y \to Y$ such that $f(s(n)) = t(f(n))$, that is, to give

$$1 + Y \xrightarrow{[y_0, t]} Y$$

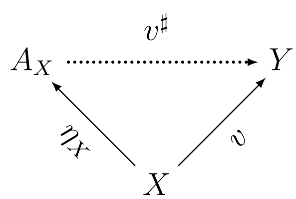
such that



Exercise A.14. Check that the diagram above commutes iff $f(0) = y_0$ and $f(s(n)) = t(f(n))$ for all $n \in \mathbb{N}$.

A.3.1 Free algebras and equations

Definition A.15 (Free algebra)**.** Let $T : \mathcal{X} \to \mathcal{X}$ and $X \in \mathcal{X}$. The free T-algebra over X is given by an algebra (A_X, α_X) and an arrow $\eta_X : X \to A_X$ such that for each algebra (Y, ν) and each $v : X \to Y$ there is a unique algebra morphism $v^\sharp : (A_X, \alpha_X) \to (Y, \nu)$ such that $v^\sharp \circ \eta_X = v$:



We say that $\mathsf{Alg}(T)$ has free algebras iff for all $X \in \mathcal{X}$ there is a free algebra over X.

Remark 1. In the case $\mathcal{X} = \mathsf{Set}$ we read this as follows: For a set of variables X there is the *term algebra* (A_X, α_X) which has as a carrier A_X all terms formed from operations in T and variables in X. η_X is the inclusion of variables into terms. v is an *assignment of variables* to elements of (Y, ν). The condition above now expresses the familiar fact that any assignment of variables v defines a unique interpretation $v^\sharp$ of terms.

Exercise A.16. Compare the definition of free algebras with the characterisation of cofree coalgebras in Exercise A.8.

We can now say that, in the case $\mathcal{X} = \mathsf{Set}$, an equation $t = t'$ of terms t, t' in variables from X is an element of $(t, t') \in A_X \times A_X$. Satisfaction of equations is then defined as follows.

Definition A.17 (Satisfaction of equations)**.** Let $T : \mathsf{Set} \to \mathsf{Set}$ and (A_X, α_X) a free T-algebra over X. Let $(Y, \nu) \in \mathsf{Alg}(T)$ and $\Phi \subset A_X \times A_X$ (ie Φ is a set of equations in variables from X). For an equation $(t, t') \in \Phi$ and an assignment $v : X \to Y$ define

$$(Y, \nu), v \models (t, t') \quad \text{iff} \quad v^\sharp(t) = v^\sharp(t')$$

We write $(Y, \nu) \models \Phi$ and say that (Y, ν) satisfies Φ, or that Φ holds in (Y, ν), iff $(Y, \nu), v \models (t, t')$ for all $(t, t') \in \Phi$ and all assignments $v : X \to Y$.

A.4 Duality

We briefly review categorical duality. A category $\mathcal{C}$ consists of a class of objects, also denoted by $\mathcal{C}$, and for all $A, B \in \mathcal{C}$ of a set of arrows (or morphisms) $\mathcal{C}(A, B)$. The *dual* (or opposite) category $\mathcal{C}^{\mathrm{op}}$ has the same objects and arrows $\mathcal{C}^{\mathrm{op}}(A, B) = \mathcal{C}(B, A)$. We write A^{op} and f^{op} for $A \in \mathcal{C}$ and $f \in \mathcal{C}(B, A)$ to indicate when we think of A as an object in $\mathcal{C}^{\mathrm{op}}$ and of f as an arrow in $\mathcal{C}^{\mathrm{op}}(A, B)$. Duality can now be formalised as follows: Let P be a property of objects or arrows in $\mathcal{C}$. We then say that

an object A (arrow f, respectively) in $\mathcal{C}$ has property co-P
iff A^{op} (f^{op}, respectively) has property P.

For example, an object A is co-initial in $\mathcal{C}$ (usually called terminal or final) iff A is initial in $\mathcal{C}^{\mathrm{op}}$; a morphism $f \in \mathcal{C}(A, B)$ is co-mono (usually called epi) iff f^{op} is mono; C is a co-product $A + B$ iff C^{op} is a product $A^{\mathrm{op}} \times B^{\mathrm{op}}$. Of particular importance for us is

Exercise A.18. Show that (E, M) is a factorisation system in $\mathcal{C}$ iff (M, E) is a factorisation system in $\mathcal{C}^{\mathrm{op}}$.

The duality principle can also be extended to functors. The dual of a functor $F : \mathcal{C} \to \mathcal{D}$ is the functor $F^{\mathrm{op}} : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}^{\mathrm{op}}$ which acts on objects and morphisms as F does. We can now state precisely that algebras are dual to coalgebras:

Proposition A.19. *Let $T : \mathcal{X} \to \mathcal{X}$. $\mathsf{Alg}(T)^{\mathrm{op}}$ is equivalent to $\mathsf{Coalg}(T^{\mathrm{op}})$.*

Proof. The iso maps objects $(TX \xrightarrow{\xi} X)^{\mathrm{op}}$ to $X^{\mathrm{op}} \xrightarrow{\xi^{\mathrm{op}}} T^{\mathrm{op}}X^{\mathrm{op}}$ and is the identity on morphisms. □

Note that the base category $\mathcal{X}$ gets dualised as well. To emphasise this trivial but important point we state an evident corollary to the proposition:

Corollary A.20. *Let $T : \mathcal{X} \to \mathcal{X}$. Then the forgetful functor $U : \mathsf{Alg}(T) \to \mathcal{X}$ is dual to the forgetful functor $U^{\mathrm{op}} : \mathsf{Coalg}(T^{\mathrm{op}}) \to \mathcal{X}^{\mathrm{op}}$.*

The fact that the base category has to be dualised makes it difficult to exploit the duality of algebras and coalgebras.

B Modal Logic

(This is Section 4 of [26].) The purpose of this chapter is to introduce modal logic as far as needed in this course. For more information see e.g. Blackburn, de Rijke, Venema [6] or Goldblatt [15].

B.1 Kripke Semantics

B.1.1 Introduction

Modal logic originated with the study of logics comprising modalities as eg 'necessarily'. In the beginning of the 20th century a piece of syntax was invented, nowadays mostly written $\Box$, in order to write formulas

$$\Box\varphi$$

having the intended meaning that φ holds necessarily. A question at that time was to describe axiomatically the valid formulas involving necessity. Different proposals were discussed generally including the following two axiom schemes and two rules.

(taut)	all propositional tautologies
(dist)	$\Box(\varphi \to \psi) \to \Box\varphi \to \Box\psi$
(mp)	from $\varphi, \varphi \to \psi$ derive ψ
(nec)	from φ derive $\Box\varphi$

The interpretation is: propositional tautologies are valid; if necessarily $\varphi \to \psi$ and necessarily φ then necessarily ψ; modus ponens is clear; if φ is valid, then necessarily φ is valid. The modal logic consisting of these axioms and rules is today usually denoted by **K**.

In general, one also proposed additional axiom schemes as eg

(refl)	$\Box\varphi \to \varphi$
(trans)	$\Box\varphi \to \Box\Box\varphi$

The interpretation is: if φ holds necessarily, then it holds indeed; if φ holds necessarily then it is necessary that it holds necessarily.

For a long time it was difficult to judge the value of such axiomatisation because there was no appropriate semantics of modal logic. This changed in the 1950s with the advent of possible worlds or Kripke semantics. The idea is to use graphs (X, R), $R \subset X \times X$, as models for modal logic and to think of X as a set of possible worlds and of R as an alternative relation. We then say that a formula holds necessarily in the world x iff it holds in all possible alternatives:

$$(X, R, x) \models \Box\varphi \quad \text{iff} \quad (X, R, y) \models \varphi \quad \text{for all } y \text{ with } xRy$$

A formula holds in (X, R) iff it holds in all worlds $x \in X$ and a formula is *valid* iff it holds in all (X, R).

Exercise B.1. If you are not familiar with Kripke semantics, then show that (dist) is valid. Also show that (nec) is correct: if φ is valid, then also $\Box\varphi$. Show that $\varphi \to \Box\varphi$ is not valid.

B.1.2 Frames and Models

We presented modal logic avoiding any discussion of propositional logic. But there is an issue: namely whether we should interpret the atomic propositions $p \in \mathsf{Prop}$ of propositional logic as variables or as constants. This distinction gives rise to the notions of Kripke frame and Kripke model.

But first let us be precise about the language of modal logic.

Definition B.2 (Modal language)**.** Given a set of atomic propositions Prop, the set of all modal formulas $\mathcal{ML}$, sometimes written $\mathcal{ML}(\mathsf{Prop})$, is defined inductively by

$$\begin{array}{lll} p \in \mathsf{Prop} & \Rightarrow & p \in \mathcal{ML} \\ \bot \in \mathcal{ML} & & \\ \varphi, \psi \in \mathcal{ML} & \Rightarrow & \varphi \to \psi \in \mathcal{ML} \\ \varphi \in \mathcal{ML} & \Rightarrow & \Box\varphi \in \mathcal{ML} \end{array}$$

$\bot$ is falsum. The other boolean operators $\top, \neg, \wedge, \vee$ can be defined from $\bot, \to$. The modal operator $\Diamond$ is defined as $\neg\Box\neg$.

If we understand atomic propositions as constants we need to extend graphs by interpretations of atomic propositions:

Definition B.3. A **Kripke model** (X, R, V) consists of a set X , a relation $R \subset X \times X$ and a valuation $V : X \to \mathcal{P}\mathsf{Prop}$.

Elements of X are called states, (possible) worlds, or points. R is called the accessibility relation or alternative relation. Elements of Prop are called atomic propositions or propositional variables.

The idea is that V assigns to $x \in X$ the set of atomic propositions holding in x; the semantics of propositional connectives is as usual and the semantics of $\Box$ is as we have seen it. To summarise:

Definition B.4 (Semantics of modal logic)**.** For a Kripke model (X, R, V) and $x \in X$ define:

$$\begin{array}{lll} (X,R,V,x) \models p & \text{iff} & p \in V(x) \\ (X,R,V,x) \not\models \bot & & \\ (X,R,V,x) \models \varphi \to \psi & \text{iff} & (X,R,V,x) \models \varphi \;\Rightarrow\; (X,R,V,x) \models \psi \\ (X,R,V,x) \models \Box\varphi & \text{iff} & xRy \;\Rightarrow\; (X,R,V,y) \models \varphi \;\text{ for all } y \in X. \end{array}$$

φ holds in a model (X, R, V), written $(X, R, V) \models \varphi$, iff $(X, R, V, x) \models \varphi$ for all $x \in X$. And φ is valid, written $\models \varphi$, iff φ holds in all models.

Notation: We write $x \models \varphi$ instead of $(X, R, V, x) \models \varphi$ when (X, R, V) is clear from the context.

We can also take another perspective on atomic propositions. Studying eg the logic of necessity, one is interested in the formulas valid under all possible interpretations of atomic propositions. We then think of atomic propositions as propositional variables:

Definition B.5. A **Kripke frame** (X, R) consists of a set X, and a relation $R \subset X \times X$. Models (X, R, V), $V : X \to \mathcal{P}\mathsf{Prop}$, are said to be *based on* (X, R) and (X, R) is called the *underlying frame* of the model.

A frame (X, R) satisfies a formula φ, or φ holds in (X, R), iff all models based on the frame satisfy φ:

$$(X, R) \models \varphi \quad \text{iff} \quad (X, R, V) \models \varphi \text{ for all } V : X \to \mathcal{P}\mathsf{Prop}$$

Note that φ holds in all models iff it holds in all frames.

One difference between models and frames is that the theory of a frame is always closed under substitution, see Exercise B.21. For frames, it is therefore enough to consider axioms as eg $\Box p \to p$ for some $p \in \mathsf{Prop}$; for models, however, we would employ an axiom scheme $\Box\varphi \to \varphi$ corresponding to the set of axioms $\{\Box\varphi \to \varphi : \varphi \in \mathcal{ML}\}$. A more essential difference between models and frames is the topic of the next

Exercise B.6. Let $p \in \mathsf{Prop}$.

1. Show that $\Box p \to p$ holds in all reflexive frames (X, R) (ie $\forall x \in X \,.\, xRx$).

2. Give an example of a non-reflexive model satisfying $\Box\varphi \to \varphi$ for all $\varphi \in \mathcal{ML}$. Is there a non-reflexive frame satisfying $\Box p \to p$?

From the point of view of logic, frames seem to be the interesting structures: When we ask what formulas are valid under all interpretations of propositional variables, it is natural to consider frames as the semantic structures for modal logic.

On the other hand, from the computer science point of view, models seem to be the natural structures. Consider a program or algorithm as given by a set of states X and a relation R, R giving for each state its successors. But program states are not just 'naked' elements, they carry additional information, typically the contents of the memory. This information can be thought of as being encoded by the valuation $V : X \to \mathcal{P}\mathsf{Prop}$. That is, thinking of modal logic as a specification language for transition systems (algorithms, programs), models are the natural semantic structures of modal logic.

But even then, the underlying frames (X, R) are of some interest. Often, we are not interested in arbitrary models (X, R, V) but want to restrict our attention to programs with special properties, eg deterministic ones. Being deterministic then, is a property of R, and hence a property of the class of underlying frames. For another typical example, think of Kripke models (X, R, V) as runs of programs. In this case we may want to require the underlying frames to have an initial state, to be reflexive, transitive, and perhaps linear.

The next section further develops the exercise above and discusses how modal logic can be used to describe certain frame classes.

B.1.3 Definability

We say that a class of frames $\mathcal{B}$ is defined by a class of formulas Φ iff $\mathcal{B} = \{(X, R) : (X, R) \models \Phi\}$. There are then two questions relating to definability:

- Given a class of formulas, can we characterise the defined class of frames?
- Given a class of frames, are there formulas defining it?

To illustrate the first question, suppose that someone proposes formulas (refl) and (trans) as axioms for necessity. Understanding then the defined class of frames would make it easier to judge the proposed axiomatisation (for example, as will be shown below, whether we accept (trans) depends on whether we think of the alternative relation as being transitive). To illustrate the second question, recall from the discussion at the end of the previous section that we might be interested in defining eg the class of deterministic frames or the class of reflexive, transitive, linear frames.

There exist only partial answers to these questions but many important cases are well-known. Table 1 gives a typical list of examples.

To check that a frame satisfying the first-order property also satisfies the modal formula is usually straight forward. If you are not familiar with this, you should do some of the correspondences in Table 1 as exercises. The converse direction is usually more difficult to establish. An easy but typical example is the case of (trans):

We show that only transitive frames satisfy $\Box p \to \Box\Box p$. Suppose (X, R) is not transitive, that is, there are $x, y, z \in X$ such that $xRy \wedge yRz \wedge \neg xRz$. We have to find a valuation V such that $(X, R, V, x) \not\models \Box p \to \Box\Box p$. Choose as extension of p the *smallest* set such that $(X, R, V, x) \models \Box p$ (ie let $p \in V(w) \;\Leftrightarrow\; xRw$). Now, $\neg xRz$ guarantees that $p \notin V(z)$ and it follows from $xRy \wedge yRz$ that $(X, R, V, x) \not\models \Box\Box p$.

B.1.4 Multimodal Logics

We have seen Kripke semantics for modal logics with one modality. But the basic ideas of modal logic and possible world semantics can be varied in many ways. We will discuss here only modal logics with more than one modality.

	Name	Axiom
1	(refl)	$\Box p \to p$
2	(trans)	$\Box p \to \Box\Box p$
3	(ser)	$\Diamond\top$
4	(det)	$\Diamond p \to \Box p$
5	(fun)	$\Diamond p \leftrightarrow \Box p$
6	(dir)	$\Diamond\Box p \to \Box\Diamond p$

	Name	Conditions on R
1	reflexive	$\forall x(xRx)$
2	transitive	$\forall x\forall y\forall z(xRy \wedge yRz \to xRz)$
3	serial	$\forall x\exists y(xRy)$
4	deterministic	$\forall x\forall y\forall z(xRy \wedge xRz \to y = z)$
5	functional	$\forall x\exists! y(xRy)$
6	directed	$\forall x\forall y\forall z(xRy \wedge xRz \to \exists x'(yRx' \wedge zRx'))$

Table 1: Modal Formulas and First-Order Correspondences

A multimodal logic has modalities $\Box_a$ for all $a \in A$ for some set A. That is, the last clause of Definition B.2 is replaced by

$$\varphi \in \mathcal{ML},\, a \in A \quad \Rightarrow \quad \Box_a\varphi \in \mathcal{ML}$$

One should now write $\mathcal{ML}(\mathsf{Prop}, A)$ but if no confusion can arise we continue to use $\mathcal{ML}$.

A frame $(X, (R_a)_{a\in A})$ for a multimodal logic has a relation R_a for each modality $\Box_a$. A model $(X, (R_a)_{a\in A}, V)$ has additionally a valuation of atomic propositions.

Example B.7 (Hennessy-Milner logic)**.** Consider a multimodal logic without atomic propositions and with modalities $\Box_a$, $a \in A$, where we think of A as a set of actions and of $\Box_a\varphi$ as 'φ holds after a'. A Kripke model is then a transition system $(X, (R_a)_{a\in A})$ (remember that there are no atomic propositions and hence no valuation). It is customary to write $x \stackrel{a}{\longrightarrow} y$ for $x\ R_a\ y$ and $[a]$ for $\Box_a$.

Example B.8 (Multi-agent systems)**.** Consider a multimodal logic with modalities $\Box_a$, $a \in A$, where we think of A as a set of agents and of $\Box_a\varphi$ as 'agent a knows φ'. Atomic propositions describe the facts agents can know. A Kripke model $(X, (R_a)_{a\in A}, V)$ can be understood as follows. X is a set of possible worlds and V describes the facts holding in each world. xR_ay means that agent a considers y as an alternative world for x. $x \models \Box_a\varphi$ means that φ holds in all worlds which are considered as alternative worlds by agent a, ie a knows φ.

Example B.9 (Temporal logic)**.** Consider a multimodal logic with two modalities $\bigcirc, \Box$ where we think of $\bigcirc\varphi$ as 'in the next state holds φ' and of $\Box\varphi$ as 'now and always in the future holds φ'. A particularly interesting Kripke frame for this logic is $(\mathbb{N}, S, \leq)$ where $m\ S\ n$ iff $n = m + 1$. Models based on this frame can be considered as runs of programs and the modal logic defined by this frame, linear temporal logic, plays an important role in the verification of programs, see eg [23, 28, 12, 35].

B.2 Bisimulation

Having seen Kripke frames and models, it is natural to ask what would be an appropriate notion of morphism for these structures. But instead of defining morphisms right away, we look first at relations between models. In particular, given two (multimodal) Kripke models $(X, (R_a)_{a\in A}, V)$, $(X', (R'_a)_{a\in A}, V')$, we are interested in describing relations $B \subset X \times X'$ such that

$$x\ B\ x' \ \Rightarrow\ (x \models \varphi \ \Leftrightarrow\ x' \models \varphi).$$

A careful analysis of the definition of $x \models \varphi$ leads to the following notion of bisimulation.

Definition B.10 (Bisimulation)**.** Given two Kripke models $(X, (R_a)_{a\in A}, V)$, $(X', (R'_a)_{a\in A}, V')$ we call $B \subset X \times X'$ a bisimulation between the models iff $x\ B\ x'$ implies that

$$\begin{aligned}
&V(x) = V(x')\\
&x \xrightarrow{a} y \ \Rightarrow\ \exists y' \,.\, x' \xrightarrow{a} y' \ \&\ y\ B\ y'\\
&x' \xrightarrow{a}{}' y' \ \Rightarrow\ \exists y \,.\, x \xrightarrow{a} y \ \&\ y\ B\ y'
\end{aligned}$$

(writing $\xrightarrow{a}$ for R_a and R'_a). x, x' are called *bisimilar* iff there is a bisimulation relating them. Bisimulations for frames can be obtained as a special case by ignoring the clause concerning the valuations V, V'.

Examples of (non-)bisimilarity can be found in the exercises. For us, the following is essential and an exercise that should not be missed.

Exercise B.11. Show by induction on the structure of formulas that given two models $(X, (R_a)_{a\in A}, V)$, $(X', (R'_a)_{a\in A}, V')$ then for all $x \in X$, $x' \in X'$ it holds: x, x' bisimilar implies that $x \models \varphi \ \Leftrightarrow\ x' \models \varphi$ for all modal formulas φ.

We now define morphisms as functional bisimulations.

Definition B.12. Given two Kripke models/frames $(X, \ldots)$, $(X', \ldots)$ a morphism $f : (X, \ldots) \to (X', \ldots)$ is a function $f : X \to X'$ such that its graph $\{(x, f(x)) : x \in X\}$ is a bisimulation.

These morphisms are usually called p-morphisms or bounded morphisms. The following observation—which should by now be no surprise—justifies to call them simply morphisms.

Proposition B.13. *The morphisms of Kripke models/frames are precisely the coalgebra morphisms.*

Proof. (Monomodal) Kripke frames are $\mathcal{P}$-coalgebras and their morphisms were shown to be functional bisimulations in Proposition A.2 (check this). Kripke models are $(\mathcal{P}\times\mathcal{P}\mathsf{Prop})$-coalgebras; multimodal Kripke frames are $\mathcal{P}(A\times -)$-coalgebras and multimodal Kripke models $(\mathcal{P}(A\times -)\times\mathcal{P}\mathsf{Prop})$-coalgebras. These cases are only slight variations. □

Another way to phrase the relationship between coalgebras and Kripke models/frames is the following:

Proposition B.14. *Let $(X,\ldots)$, $(X',\ldots)$ be two Kripke models/frames. Then $x\in X$, $x'\in X'$ are bisimilar (in the sense of modal logic) iff they are behaviourally equivalent (in the coalgebraic sense).*

The relationship between modal formulas and morphisms is summarised by the following two classical results. We need some standard terminology: a formula φ is preserved under quotients if $A\to A'$ surjective and $A\models\varphi$ implies $A'\models\varphi$; φ is preserved under submodels/subframes if $A'\to A$ injective and $A\models\varphi$ implies $A'\models\varphi$; φ is preserved under disjoint unions (or coproducts) if $A_i\models\varphi$ for all $i\in I$ implies $\coprod_I A_i\models\varphi$; φ is preserved under domains of quotients if $A'\to A$ surjective and $A\models\varphi$ implies $A'\models\varphi$.

Proposition B.15. *Wrt Kripke models, modal formulas are preserved under quotients, submodels, disjoint unions, and domains of quotients.*

Proposition B.16. *Wrt Kripke frames, modal formulas are preserved under quotients, subframes, and disjoint unions.*

The proof of this propositions is an easy corollary to Exercise B.11.

B.3 The Logic of Bisimulation

The aim of this section is to substantiate the claim that modal logic is the logic of bisimulation. We have seen in Exercise B.11 that for two models (X,R,V), (X',R',V'), and $x\in X$, $x'\in X'$

$$x,x' \text{ bisimilar} \quad\Rightarrow\quad \forall\varphi\in\mathcal{ML}: x\models\varphi \;\Leftrightarrow\; x'\models\varphi,$$

that is, bisimilarity implies modal equivalence. Unfortunately, the converse does not hold. Figure 1 shows an example where x has for each $n\in\mathbb{N}$ a branch of length n, and x' has additionally an infinite branch. That x and x' are not bisimilar is not difficult to see:

Figure 1: Modally equivalent but not bisimilar models

Exercise B.17. Consider the models in Figure 1 (assume that all states satisfy the same atomic propositions). Show that x, x' are not bisimilar.

To show that x and x' are modally equivalent is not difficult either but requires a bit more work, see Exercise B.25.

The example suggests (at least after having done Exercise B.25) that the failure of modal logic to characterise states up to bisimilarity is related to the facts that

- a single modal formula can not express enough about an infinite branch, and that
- a transition system may have infinite branching.

And indeed, adjusting either of the two points above results in a perfect match of bisimilarity and modal expressiveness. This is the contents of the following two theorems.

The first idea is to increase expressiveness of modal logic using infinitary modal logic $\mathcal{ML}_\infty$. $\mathcal{ML}_\infty$ is defined as $\mathcal{ML}$ with the additional clause

$$\Phi \subset \mathcal{ML}_\infty \quad \Rightarrow \quad \bigwedge \Phi \in \mathcal{ML}_\infty$$

and stipulating $\quad x \models \bigwedge \Phi \Leftrightarrow \forall \varphi \in \Phi : x \models \varphi.$

Theorem B.18. *For each model (X, R, V) and each $x \in X$ there is a formula $\varphi_x \in \mathcal{ML}_\infty$ such that for all models (X', R', V') and all $x' \in X'$*

$$x' \models \varphi_x \quad \textit{iff} \quad x, x' \textit{ bisimilar.}$$

The other idea is to restrict attention to models with finite branching.

Theorem B.19 (Hennessy and Milner)**.** *Let K be the class of image-finite Kripke models, ie for all (X, R, V) and all $x \in X$ the set $\{y : x \; R \; y\}$ is finite. Then for all (X, R, V), (X', R', V') in K and all $x \in X$, $x' \in X'$*

$$\forall \varphi \in \mathcal{ML} : x \models \varphi \Leftrightarrow x' \models \varphi \Rightarrow x, x' \textit{ bisimilar.}$$

From the point of view of classical first-order logic, however, the most satisfactory explanation of the relationship of modal logic to bisimulation is the following characterisation of modal logic as the bisimulation invariant fragment of first-order logic: A first-order formula is invariant under bisimulations iff it is equivalent to a modal formula.

To make this precise we note that a Kripke model (X, R, V) can also be understood as a first-order model with one binary relation R and one unary predicate P for each atomic proposition $p \in \mathsf{Prop}$. Let us call $\mathcal{FL}$ the corresponding first-order language (containing one relation symbol and for each atomic proposition a unary predicate symbol). The definition of $(X, R, V, x) \models \varphi$ in Section B.1.2 can now be read as a translation $(-)^* : \mathcal{ML} \to \mathcal{FL}$ of modal formulas in first-order formulas with one free variable x:

$$\begin{aligned}
p^* &= P(x) \\
\bot^* &= \bot \\
(\varphi \to \psi)^* &= \varphi^* \to \psi^* \\
(\Box\varphi)^* &= \forall y : xRy \to \varphi^*[y/x]
\end{aligned}$$

where y is a variable not occurring free in φ^* (and $[y/x]$ denotes substitution of y for x).

Theorem B.20 (van Benthem)**.** *A first-order formula $\psi \in \mathcal{FL}$ is invariant under bisimulation iff it is logically equivalent to a translation φ^* of a modal formula $\varphi \in \mathcal{ML}$.*

B.4 Exercises

Exercise B.21. Show that the theory of a frame is closed under substitution. That is, for $\varphi, \psi \in \mathcal{ML}$ and $p \in \mathsf{Prop}$ it holds that $(X, R) \models \varphi \;\Rightarrow\; (X, R) \models \varphi[\psi/p]$ (where $[\psi/p]$ denotes substitution of ψ for p).

Exercise B.22 (Examples of bisimilarities)**.** Assume a monomodal language. Show that in the models given below the states x and x' are bisimilar.

1. The relational structure of the models is depicted below. For the valuations assume that $V(y) = V(z) = V'(y')$ and $V(x) = V'(x')$.

2. For the following models assume that all states have the same valuation.

Exercise B.23 (A non-example of bisimilarity)**.** Assume a multimodal language with three modalities $A = \{a, b, c\}$ and no atomic propositions. Consider the two models below.

1. Show that x, x' are not bisimilar.
2. Give modal formulas that distinguish x and x'.

Note that both models show the same behaviour $\{ab, ac\}$ if only traces are considered.

Exercise B.24 (Bisimilarity of frames)**.** For frames bisimilarity does not imply modal equivalence. First note that x, x' in the the following two *frames* are bisimilar.

Now, show

1. $x \models \varphi \;\Rightarrow\; x' \models \varphi$
2. $x' \models \varphi \not\Rightarrow x \models \varphi$

Exercise B.25 (Modal equivalence does not imply bisimilarity)**.** Denote by (X, R, V) and (X', R', V') the two models of Figure 1. The aim is to show that x and x' are modally equivalent. We need two definitions.

The depth of a modal formula counts the number of nested boxes, ie $\mathit{depth}(\bot) = \mathit{depth}(p) = 0$, $\mathit{depth}(\varphi \to \psi) = \max(\mathit{depth}(\varphi), \mathit{depth}(\psi))$, $\mathit{depth}(\Box\varphi) = \mathit{depth}(\varphi) + 1$.

Denote by $\mathit{Cut}(x, n)$ the model which is obtained from (X, R, V) by deleting all states which are not reachable from x in n or fewer than n steps. For example $\mathit{Cut}(x, 0)$ consists just of x. Similarly define $\mathit{Cut}'(x', n)$.

1. Show that $\mathit{depth}(\varphi) \leq n$ implies that $(\mathit{Cut}(x, n), x) \models \varphi \;\Leftrightarrow\; (X, R, V, x) \models \varphi$ and that $(\mathit{Cut}'(x', n), x') \models \varphi \;\Leftrightarrow\; (X', R', V', x') \models \varphi$.
2. Conclude that for all modal formulas $(X, R, V, x) \models \varphi \;\Leftrightarrow\; (X', R', V', x') \models \varphi$.

B.5 Notes

For background on modal logic the reader is referred to Chapter 2 and 3 of Blackburn, de Rijke, Venema [6]. We just note that bisimulation goes back, in its functional form, to Segerberg [34], and in its relational form to van Benthem [37]; Theorem B.18 can be found in Barwise and Moss [5], Theorem B.19 is due to Hennessy and Milner [17], and Theorem B.20 to van Benthem [37, 38].

C Proofs and Answers to Exercises

Theorem 2.7 The categories $\mathsf{Fin}^{\mathrm{op}}$ and $\mathsf{BA}_{\mathsf{fin}}$ are equivalent.

Proof. We have to show that $e : A \to PSA$ is an isomorphism of Boolean algebras for all finite $A \in \mathsf{BA}$. First, e is a homomorphism because e is induced by homming into a dualising object.

e injective: We have to show that if $a \not\leq b$, then there is a point $p : A \to \mathbb{2}$ such that $pa = 1$ and $pb = 0$. Define $pc = 1$ for all $c \geq a$. Check that p is a BA-morphism.

e surjective: Let $p : A \to \mathbb{2}$ be a BA-morphism. Show that there is $a \in A$ such that $pb = 1$ iff $b \geq a$ and that a is an atom. Conclude that $p = \hat{a}$. □

References

[1] S. Abramsky. Domain theory in logical form. *Ann. Pure Appl. Logic*, 51, 1991.

[2] S. Abramsky and A. Jung. Domain theory. In *Handbook of Logic in Computer Science*. OUP, 1994.

[3] P. Aczel and N. P. Mendler. A final coalgebra theorem. In *Category Theory and Computer Science*, volume 389 of *LNCS*, 1989.

[4] A. Baltag. A logic for coalgebraic simulation. In *CMCS'00*, ENTCS 33, 2000.

[5] J. Barwise and L. Moss. *Vicious Circles*. CSLI, 1996.

[6] P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*. CUP, 2001.

[7] M. M. Bonsangue. *Topological Dualities in Semantics*. PhD thesis, Vrije Universiteit Amsterdam, 1996.

[8] C. Brink and I. M. Rewitzky. *A Paradigm for Program Semantics: Power Structures and Duality*. Cambridge University Press, 2001.

[9] A. Chagrov and M. Zakharyaschev. *Modal Logic*. Clarendon Press, 1997.

[10] C. Cîrstea. On specification logics for algebra-coalgebra structures: Reconciling reachability and observability. In *FoSSaCS'02*, LNCS 2303, 2002.

[11] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. CUP, 1990.

[12] E.A. Emerson. Temporal and modal logic. In *Handbook of Theoret. Comput. Sci.*, volume 1. Elsevier, 1990.

[13] J. Font, R. Jansana, and D. Pigozzi. A survey of abstract algebraic logic. *Studia Logica*, 74, 2003.

[14] R. Goldblatt. Metamathematics of modal logic I. *Reports on Mathematical Logic*, 6, 1976.

[15] R. Goldblatt. *Logics of Time and Computation*, volume 7 of *CSLI Lecture Notes*. CSLI, 1992. Second Edition.

[16] R. Goldblatt. A calculus of terms for coalgebras of polynomial functors. In *CMCS'01*, ENTCS 44, 2001.

[17] M. Hennessy and R. Milner. Algebraic laws for nondeterminism. *Journal of the Association for Computing Machinery*, 32, 1985.

[18] B. Jacobs. Many-sorted coalgebraic modal logic: a model-theoretic study. *Theor. Inform. Appl.*, 35, 2001.

[19] P. Johnstone. *Stone Spaces*. Cambridge University Press, 1982.

[20] B. Jónsson and A. Tarski. Boolean algebras with operators, part 1. *Amer. J. Math.*, 73, 1951.

[21] B. Jónsson and A. Tarski. Boolean algebras with operators, part 2. *American Journal of Mathematics*, 74, 1952.

[22] M. Kracht. *Tools and Techniques in Modal Logic*. Elsevier, 1999.

[23] F. Kröger. *Temporal Logic of Programs*. Springer, 1987.

[24] C. Kupke, A. Kurz, and D. Pattinson. Algebraic semantics for coalgebraic logics. In *CMCS'04*.

[25] C. Kupke, A. Kurz, and Y. Venema. Stone coalgebras. In *CMCS'03*, volume 82 of *ENTCS*, 2003.

[26] A. Kurz. *Coalgebras and Modal Logic - Course Notes for ESSLLI 2001*. University of Helsinki, 2001.

[27] A. Kurz and A. Palmigiano. Coalgebras and modal expansions of logics. In *CMCS'04*, ENTCS 106, 2004.

[28] Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems*. Springer, 1992.

[29] L. Moss. Coalgebraic logic. *Ann. Pure Appl. Logic*, 96, 1999.

[30] A. Palmigiano. A coalgebraic semantics for positive modal logic. In *CMCS'03*, ENTCS, 2003.

[31] D. Pattinson. Semantical principles in the modal logic of coalgebras. In *STACS'01*.

[32] M. Rößiger. Coalgebras and modal logic. In *CMCS'00*.

[33] J. Rutten. Universal coalgebra: A theory of systems. *Theor. Comp. Sci.*, 249, 2000.

[34] K. Segerberg. An essay in classical modal logic. *Filosofiska Studier 13*, 1971.

[35] C. Stirling. Modal and temporal logics. In *Handbook of Logic in Computer Science*, volume 2. Oxford University Press, 1992.

[36] M. H. Stone. The theory of representations for boolean algebras. *Trans. Amer. Math. Soc*, 40, 1936.

[37] J. van Benthem. *Modal Correspondence Theory*. PhD thesis, University of Amsterdam, 1976.

[38] J. van Benthem. *Modal Logic and Classical Logic*. Bibliopolis, 1983.

[39] S. J. Vickers. *Topology Via Logic*. CUP, 1989.

[40] W. Wechler. *Universal Algebra for Computer Scientists*, volume 25 of *EATCS Monographs on Theor. Comp. Sci.* Springer, 1992.